New-type digital signature system and device

Patent number:	CN1256463
Publication date:	2000-06-14
Inventor:	ZHAO FENGGUANG (CN); NI XINGFANG (CN)
Applicant:	ZHAO FENGGUANG (CN)
Classification:	
- international:	***G06F17/16;*** **G06F17/16;** (IPC1-7): G06F17/16
- european:	
Application number:	CN19990124110 19991125
Priority number(s):	CN19990124110 19991125

Report a data error here

Abstract of **CN1256463**

Along with the development of electronic business, digital signature technology becomes important increasingly. The present invention proposes one completely new signature system capable of preventing decoding and forging based on that the coupled integral indefinite equations are hard to solve. The signature system has randomness similar to DSS, so that it can prevent forging effectively. Furthermore, the device of the present invention relates to only additive operation and multiplying operation and thus is suitable for being integrated and developed in DSP.

---

[19]中华人民共和国国家知识产权局

[51]Int.Cl[7]
G06F 17/16

[12]发明专利申请公开说明书

[21]申请号 99124110.X

[43]公开日 2000年6月14日

[11]公开号 CN 1256463A

[22]申请日 1999.11.25 [21]申请号 99124110.X

[71]申请人 赵风光
地址 200434 上海市水电路1324弄9支弄9号102室
共同申请人 倪兴芳
[72]发明人 赵风光 倪兴芳

权利要求书1页 说明书3页 附图页数1页

[54]发明名称 一种新型数字签名体制和装置

[57]摘要

随着电子商务的发展,数字签名技术受到了越来越普遍的重视。本发明利用数 字规划中整数不定方程组求解的困难提出了一种全新的数字签名体制,参见附图。该体制防止破译与伪造的依据是整数不定方程组的求解在计算上是强NP问题。本发明的签名体制具有类似于DSS的随机特性,有效地防止了伪造签 名的可能性;更进一步,本发明由于只涉及算术加法和乘法运算,因此更 易于硬件集成,特别适宜于数字信号处理器DSP上的开发。

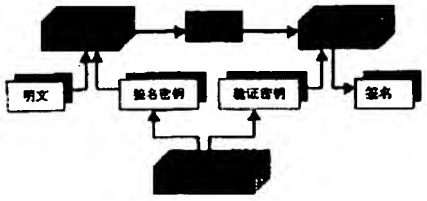

图1 数字签名体制功能模块流程

ISSN1008-4274

权力要求书

1. 一种有限数字签名体制，使用户把电子数据转换为签名信息. 该体制包含一个签名密钥，一个验证密钥，一个有限签名算法与验证算法. 其特征在于签名密钥是一个整数矩阵 A，验证密钥是两个整数矩阵 B 和 C，满足 $AB = C$. 有限签名算法对电子数据信息 x 做矩阵向量积 $y = xA$. 验证算法只需计算两个矩阵向量积 yB 和 xC，并比较结果 yB 是否等于 xC.
2. 一种无限数字签名体制，使用户把电子数据转换为签名信息. 该体制包含一个签名密钥，一个验证密钥，一个密钥生成算法，一个无限签名算法与验证算法. 其特征在于密钥生成算法从对角阵出发，执行一系列随机的初等变换，相应变换过程作为签名密钥，同时输出二个整数矩阵作为验证密钥. 无限签名算法是对电子数据信息做一系列矩阵的初等变换，再产生一个随机向量并与变换结果一起合成一个新向量，对新向量再做一系列矩阵的初等变换，得到签名信息. 验证算法只需计算两个矩阵向量积，并比较结果.
3. 如上述权利要求 1 和 2 所述之体制，所有运算是有限位整数，更包含一个溢出控制系统，该系统对所有算术运算做溢出检测. 还包含一个伪随机数生成算法，以控制产生密钥的随机性.
4. 一种有限数字签名程序，使用户把电子数据转换为签名信息. 该程序包含一个签名密钥，一个验证密钥，一个有限签名程序与验证程序. 其特征在于签名密钥是一个整数矩阵 A，验证密钥是两个整数矩阵 B 和 C，满足 $AB = C$. 有限签名程序对电子数据信息 x 做矩阵向量积 $y = xA$. 验证程序只需计算两个矩阵向量积 yB 和 xC，并比较结果 yB 是否等于 xC.
5. 一种无限数字签名程序，使用户把电子数据转换为签名信息. 该程序包含一个签名密钥，一个验证密钥，一个密钥生成程序，一个无限签名程序与验证程序. 其特征在于密钥生成程序从对角阵出发，执行一系列随机的初等变换，相应变换过程作为签名密钥，同时输出二个整数矩阵作为验证密钥. 无限签名程序是对电子数据信息做一系列矩阵的初等变换，再产生一个随机向量并与变换结果一起合成一个新向量，对新向量再做一系列矩阵的初等变换，得到签名信息. 验证程序只需计算两个矩阵向量积，并比较结果.
6. 如上述权利要求 4 和 5 所述之程序，所有运算是有限位整数，更包含一个溢出控制程序，该程序对所有算术运算做溢出检测. 还包含一个伪随机数生成程序，以控制产生密钥的随机性.
7. 一种有限数字签名装置，使用户把电子数据转换为签名信息. 该装置包含一个签名密钥，一个验证密钥，一个有限签名装置与验证装置. 其特征在于签名密钥是一个整数矩阵 A，验证密钥是两个整数矩阵 B 和 C，满足 $AB = C$. 有限签名装置对电子数据信息 x 做矩阵向量积 $y = xA$. 验证装置只需计算两个矩阵向量积 yB 和 xC，并比较结果 yB 是否等于 xC.
8. 一种无限数字签名装置，使用户把电子数据转换为签名信息. 该装置包含一个签名密钥，一个验证密钥，一个密钥生成装置，一个无限签名装置与验证装置. 其特征在于密钥生成装置从对角阵出发，执行一系列随机的初等变换，相应变换过程作为签名密钥，同时输出二个整数矩阵作为验证密钥. 无限签名装置是对电子数据信息做一系列矩阵的初等变换，再产生一个随机向量并与变换结果一起合成一个新向量，对新向量再做一系列矩阵的初等变换，得到签名信息. 验证装置只需计算两个矩阵向量积，并比较结果.
9. 如上述权利要求 7 和 8 所述之装置，所有运算是有限位整数，更包含一个溢出控制装置，该程序对所有算术运算做溢出检测. 还包含一个伪随机数生成装置，以控制产生密钥的随机性.

说　明　书

一种新型数字签名体制和装置

本发明属于密码学和计算机安全等技术领域，是一种利用数学中的 NP 问题实现数字签名的数据处理方法及其器件.

随着电子商务的发展，数字签名技术受到了越来越普遍的重视. 保护电子信息的完整性，特别是保护重要信息的完整，已成为国际社会普遍关心的重大问题. 数字签名技术是一种保证电子数据不可更改的公开密钥体制，该密钥体制需要两个数学上配对的密钥，一个私有密钥用于对电子数据的签名，因此也称为签名密钥；一个公开密钥用于对电子数据的签名验证，因此也称为验证密钥.

第一个切实可行的公开密钥算法是由芮沃斯特，沙米尔和阿当蔓提出的，这就是著名的 RSA 公开密钥体制，该体制基于数学中的大数分解困难. 精确地说，假设 p，q 是二素数，$n = pq$. 当 n 足够大时，由 n 得出 p 和 q 在数学上是困难的，因此 p 和 q 是该体制中的秘密. 一旦我们找到了快速的大数分解方法，该体制将完全崩溃. 该体制的特点是即既可用于数字签名又可用于数据加密，其签名和加密是对称的互逆过程. 该算法的专利权由 RSA 数据安全公司所持有，其终止期限为 2000 年末. 事实上目前的很多商业产品均基于该体制. 但是，该体制有一些致命的缺陷：由于大数因子分解的新成就，导致该体制所采用的数学运算位数越来越长. 数学运算的位数过长导致硬件开发的困难，并且硬件产品的开发寿命大大降低. 另外其签名和加密的对称性一直是密码学家争论的焦点，这也是导致美国政府未能将其纳入数字签名标准的原因.

目前，能够取代 RSA 并在公开网络中传送密钥的是由戴费和海尔曼提出的密钥交换算法，简称为 DH 密钥交换体制. 该体制保证安全的手段在于数论中离散对数问题的困难. 精确地说，假设 p 是一个位数很长的素数，a 是数域 p 中的本元素，通过执行如下协议就可以在用户二端产生一把共享密钥.

- A 选择一个大于零小于 p 的随机数 v_A；
- A 计算 $u_A = \exp(v_A)$.
- B 选择一个大于零小于 p 的随机数 v_B
- B 计算 $u_B = \exp(v_B)$.
- A 传送 u_A 给 B； B 传送 u_B 给 A；
- A 计算 $K = \exp(u_B)$； B 计算 $K = \exp(u_A)$.

这里 $\exp(x)$表示 $a^x \bmod p$. 容易验证：A 和 B 最后一步所得到的 K 值是相同的，因此该数可以成为 A 和 B 之间的共享密钥. 著名的软件产品 PGP 的最新版就是采用了这种策略，以取代 RSA,来实现 Email 用户之间的数据传送. 目前该算法被认为比 RSA 更安全.

1984 年，爨盖米尔提出了一种全新的数字签名方法以取代 RSA 数字签名方法，该算法的安全措施也是基于离散对数问题的困难，同时还引进了一种随机化安全措施以避免签名被伪造的可能性，正因为这个原因，美国政府采用了该算法的一个修正形式作为美国的数字签名标准，即 DSS 或 DSA.

近年来，在公开密钥系统的研究中，人们采用背包问题，椭圆曲线方法以及 LUCAS 函数. 但是几乎所有基于背包问题的公开密钥系统都被破译了，而后二者似乎比 RSA 方法更安全. 目前大部份安全公开密钥系统都是基于数论的 NP 问题，但这些系统的公有特点是：所使用的数学运算位数过长（1024 或 2048 位加减乘除），从而导致软件运行速度缓慢，硬件开发困难的不利局面.

发明简要：本发明基于整数线性不定方程 $Ax = b$ 求解的困难．可以证明，该问题是强 NP 问题，也就是说不存在能在多项式时间内找出它的解的任何算法．基于这个前题，我们选择整数矩阵 A，其大小为 N 行 M 列；整数矩阵 B，其大小为 M 行 N 列；整数矩阵 C，其大小为 N 行 N 列；使满足 $AB = C$．对签名运算，公开 B 和 C，这也就是所谓的公开密钥或验证密钥，A 作为签名密钥不公开．对于一个大小为 N 的信息 x，其签名为 $xA = y$，则 y 成为对 x 的合法签名．验证该签名的合法性只需要简单地判断，yB 是否等于 xC.

该算法可能存在的缺陷是随签名次数增加，有可能回解出签名密钥 A. 为此我们又引进了一个随机机制，即在签名矩阵 A 中参与一些随机比特．这样既可以避免 A 被重构，又可以防止使用二段已知签名伪造一个假签名的可能性.

本发明所涉及的运算都可以使用 3 2 位或 6 4 位的整数运算，如果采用更加精巧的构造，甚至可以避免整数除法运算，因此可以非常方便地开发硬件产品.

无论使用 32 位或 64 位运算，该签名体制都必须有一个强有力的位溢出控制算法，该算法将对所有的数学运算实行位溢出检测.

本发明还给出了产生密钥的算法，该算法从对角阵出发，经一系列矩阵初等变换得到签名和验证所需要的密钥.

发明细节：在数学上已经证明，整数矩阵方程 $AB = C$ 是强 NP 问题，也就是说不存在能在多项式时间内找出它的解的任何算法，这里整数矩阵 A 的大小为 N 行 M 列；整数矩阵 B 的大小为 M 行 N 列；整数矩阵 C 的大小为 N 行 N 列. 利用这一点，我们可以很容易地构造一个有限签名算法，其细节如下:

有限签名算法

输入大小为 N 的签名信息 x

- 随机产生矩阵 A 和 B，其中 A 为 N 行 M 列，B 为 M 行 N 列
- 计算 $C = AB$，并公开 B 和 C
- 计算 $y = xA$

则 y 就是 x 的签名信息. 验证 y 的合法性，只须简单地计算 yB 是否等于 xC. 因此 B 和 C 就是所谓的验证密钥，A 则是签名密钥. 对于只需要有限个签名的应用环境，该算法是相对安全的. 一旦签名次数增加，有个可能利用原始信息和签名信息重构 A；另一方面，有可能利用旧的签名伪造一个假签名，因为上述签名过程是线性的. 为此，我们将使用初等变换的办法，由此可以得到更加灵活和安全的无限签名算法。

为描述方便，本部分总假设 $M = 2N$. 这样作有助于把矩阵分解成同样尺寸的块，而方阵形式是最容易处理的. 根据矩阵论的基本原理，任何一个整数矩阵都可利用初等变换转化为对角阵；因此构造合适的矩阵作为以上描述的签名矩阵，可以从对角阵出发，经一系列初等变换得到.

对于 A，B，C 的构造，我可首先将其分块为 $A = (A_1, A_2)$，$B = (B_1, B_2)$，$C = (C_1)$，这里所有块矩阵都是 N 行 N 列的方阵. 由于 $AB = C$，因此

$$A_1B_1 + A_2B_2 = C_1 \tag{1}$$

为了构造这些矩阵，我们从对角阵 $D_A^1, D_B^1, D_A^2, D_B^2, D_C^1$ 出发，它们应满足：

$$D_A^1 D_B^1 + D_A^2 D_B^2 = D_C^1 \tag{2}$$

假设上述对角阵经过了 w 个左初等变换，记为 $P_L^1, P_L^2, \ldots P_L^w$，和 t 个右初等变换 $P_r^1, P_r^2, \ldots P_r^t$ 及 s 个中初等变换，记为 $P_c^1, P_c^2, \ldots P_c^s$，得到了 A，B，C。则

$$A = P_L^1 P_L^2 \ldots P_L^w (D_A^1, D_A^2) P_C^1 P_C^2 \ldots P_C^t \tag{3}$$

$$B = \underline{P_C^1}\underline{P_C^2} \cdots \underline{P_C^t}\ (D_B^1,\ D_B^2)\ P_r^1 P_r^1 \cdots P_r^t \tag{4}$$

$$C = P_L^1 P_L^2 \cdots P_L^w\ (C_1)\ P_r^1 P_r^2 \cdots P_r^s \tag{5}$$

其中，$\underline{P_C^t}$是 P_C^t的逆阵，$i = 1 \ldots t$. 由此算出的 B，C 可以公开做为验证密钥，但是我们需要存储 A 的所有分解信息，以便签名时更加灵活。上述推导可用如下的密钥生成算法来描述

密钥生成算法

- 随机选取对角阵 D_A^1，D_B^1
- 计算 $C_1 = D_A^1 D_B^1$，令 $D_B^2 = 0$
- 随机产生初等阵 $P_C^1 P_C^2 \cdots P_C^t$, $P_L^1 P_L^2 \cdots P_L^w$, $P_r^1 P_r^2 \cdots P_r^s$
- 利用(4)和(5)，计算 B 和 C 并公开.
- 存储 D_A^1, $P_C^1 P_C^2 \cdots P_C^t$, $P_L^1 P_L^2 \cdots P_L^w$ 作为私有密钥

利用以上产生的密钥，可以得到如下的签名算法

无限签名算法

输入大小为 N 的签名信息

- 计算 $u = x P_L^1 P_L^2 \cdots P_L^w D_A^1$
- 产生大小为 N 的随机数 v
- 计算 $y = (u, v)^T P_C^1 P_C^2 \cdots P_C^t$

则 y 就是 x 的签名信息. 验证 y 的合法性，只须简单地计算 yB 是否等于 xC. 由此可以看出，该签名体制在计算上是相当简单的. 它首先对待签名的数据做一系列初等变换，再产生一个随机向量并与变换结果一起合成一个新向量，对新向量再做一系列矩阵的初等变换，得到相应的签名信息.

硬件描述： 该发明的实现需要借助于一个物理实体，该实体可能是一台 PC 机或者是一个专用芯片. 这个实体至少包含四个部件，即存储器③，中央处理器②，密钥生成器⑥和随机发生器⑦. 如附图 1 所示.

存储器③用来存储该体制的处理代码和运算过程中的动态数据. 中央处理器②则执行该密码体制的运算代码. 因此它必须包含至少一个累加器，至少一个乘法器和多个其他功能的寄存器，同时还应有一个与外存交换数据的物理接口. 在签名之前还需要产生与之相关的钥匙分量，因此还须要一个密钥生成器⑥. 该生成器在处理过程中，需要用到随机数，因此还必须有一个随机数发生器⑦. 该器件可以是物理的，也可以是软件模拟的. 如果采用后者，则该器件可以去掉，但需要增加存储器的容量和运算代码. 本发明装置的输入为明文信息①，输出与明文相对应签名信息④.

该装置的签名过程是对明文信息做一系列矩阵的初等变换，产生一个随机向量并与变换结果一起合成一个新向量，对新向量再做一系列矩阵的初等变换，得到签名信息. 该装置的验证过程只需计算两个矩阵向量积，再比较结果. 该装置的加密过程只须简单地计算向量和矩阵的积；解密过程需要首先做一系列矩阵的初等变换，求解一个对角整数方程组，再做一系列矩阵的初等变换，得到明文信息.

密钥生成器则需要从对角阵出发，执行一系列随机的左中右初等变换，输出相应变换细节作为签名密钥，同时输出二个整数矩阵作为验证密钥⑤.

本装置可以做专用签名工具，以保证电子信息的数据完整. 由于其硬件设计的简单和方便，必将成为电子商务安全中一个有竞争力的候选者.

说明书附图

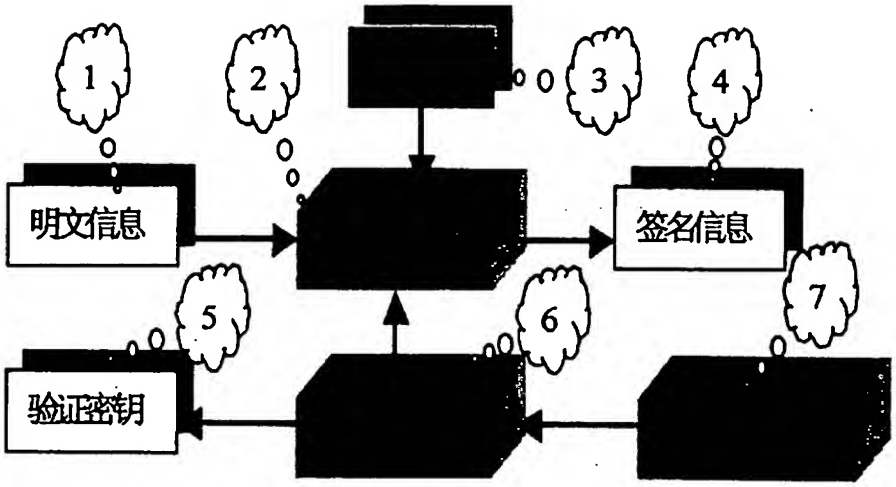

图 1: 发明装置功能模块流程